4

EXPLOITING SOFTWARE DIVERSIFICATION FOR WEBASSEMBLY

4.1 Offensive Diversification: Malware evasion

TODO The malware evasion paper

4.1.1 Objective

Test and evade the resilience of WebAssembly malware detectors mentioned in Subsection 2.1.5.

4.1.2 Approach

TODO We use wasm-mutate **TODO** How do we use it? **TODO** Controlled and uncontrolled diversification.

4.1.3 Results

4.2 Defensive Diversification: Speculative Side-channel protection

TODO Go around the last paper

---

[0] Comp. time 2023/10/03 14:21:42

4.2.1 Threat model

- Spectre timing cache attacks.
    - Rockiki paper on portable side channel in browsers.

4.2.2 Approach

- Use of wasm-mutate

4.2.3 Results

- Diminshing of BER